Title: Managing Risk to Critical Infrastructures at the National Level
Transcript

Part 1: Critical Infrastructures and Their Reliance on Critical Information Infrastructures

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and executive outreach. Today I'm pleased to introduce Bradford Willke, who's responsible for leading CERT's efforts in information security assessment and evaluation. Today we'll be discussing how to establish a national risk management program for critical information infrastructures. So welcome Bradford, glad to have you with us today.

Bradford Willke: Thanks Julia, it's really great to be talking with you.

Julia Allen: So let me get us started. Addressing critical information infrastructures at the national level can be a pretty challenging undertaking. So in your travels and observations, what are some of the key critical infrastructures for most countries? And a companion question is what types of organizations are typically involved in operating those infrastructures?

Bradford Willke: Right, so I think everybody can sort of look around and see the critical infrastructures they rely on day to day as a consumer, in their own society. And we're talking about water or electricity, telecommunications. These days no one really talks about telecom and information without citing the Internet. So those sort of foundational things – even transportation systems, manufacturing, the sort of large logistical infrastructures are what we're talking about when we say critical.

When we start talking about organizations that are involved, a lot of us point to the government, I think because they're typically organizing efforts to protect or define what is critical infrastructure, from their vantage point in citing and writing policies, standards, regulations. But I also think we have to consider the entire gamut of, down to owners and operators, standards, communities. I think we can also consider that citizens' perspective as somebody who is a consumer of those operations of critical infrastructures are also in the mix when we define owners, operators and some of the influence relationships.

Julia Allen: So it sounds like you've got all kinds of players in this arena. You've got government players at the federal, state, local level. You have private sector organizations that certainly own and operate a great part of that. And then you've got all of us as consumers and users, right?

Bradford Willke: That's right. And I think, again, you hit the nail on the head with the bulk of the critical infrastructure being owned and operated out there, residing in, not in federal hands. Federal hands certainly cover the governance aspects, the policy aspects, but if you look at the U.S. National Infrastructure Protection Plan, we're talking about 80 to 85% of critical infrastructure in the hands of private industry and private organizations.

Julia Allen: So I know that in some of our conversations you draw a distinction between critical infrastructure protection and critical information infrastructure protection – it's kind of a little bit of a

mouthful. But could you kind of just highlight what the differences are between the two and why the distinction is important?

Bradford Willke: Sure. Well let's start off with the easy one. I think critical infrastructure protection would deal with those large sectors of infrastructure. Again, if we look at just energy and we break that down into distribution, transmission, generation of power – and that's only one segment of energy. If you look at energy and its contribution to societal goals, as well as national goals led by a government, and that's to provide for a public good – national security, economic stability, feelings of wellness and wellbeing, meaning a public psychology, if you will. And I think when we consider that there are probably 10 or so critical infrastructures in most nations, we can readily identify those things.

Critical information infrastructure protection runs a different line of thought. And that is within those critical infrastructures, which are generally divided again into sectors – numbering between, around 10 but between 10 and 17 in some cases – we would look at the owners and operators, the facilitators of those sectors, and we would find the information infrastructures below that, that help facilitate, for instance, electronic delivery or gas and petroleum distribution. We might look at water systems and water treatment facilities and look at the supervisory control and data acquisition systems, or SCADA. We might look for information systems at that level that support that infrastructure's contribution to the public good.

Julia Allen: So would it be fair to say that the information infrastructure aspect – sometimes we'll call that the IT Infrastructure – but I also get the sense that sometimes the information infrastructure, because of the information that has to be exchanged, can actually span critical infrastructures. Is that correct?

Bradford Willke: It can. And again if you look at the U.S. example – and I don't think we have to uniquely talk about the U.S. but it's something I know well – the U.S. example is that not only are there 17 sectors, one of them being IT, another one being telecommunications, but within the IT sector we're really talking about the ability of the United States to purchase or to build software, to facilitate web services, to provide the underpinnings and foundations of the Internet. And those are what the technology sector would deem critical infrastructure or key resources.

And I think, yes, you can say that the Internet and SCADA systems are a critical information infrastructure, but I think you discount then the reliance on other infrastructures – agriculture, transportation, manufacturing – and their dependency on infrastructures as well. And I also think you discount this notion of interdependency, which is a concept that is sort of unique to critical infrastructure protection and critical information infrastructure protection, at a computer system and network level.

Part 2: National Risk Management Frameworks and Public/Private Partnerships

Julia Allen: Well I tell you that's kind of a nice segue into my next question which is how we get our heads around this whole arena or set of topics from a risk management perspective, because when you talk about interdependencies, clearly you've got risks within the infrastructure itself. But then you've got, as you were starting to describe, some of these interdependencies where technology and information flow kind of serves as an underpinning. So how can we tackle all of this from a, think about this as a risk issue or a problem of risk management?

Bradford Willke: Yes, I think there's some good frameworks to look at, and these are mostly internationally formed. But I think nations have arrived at these things and some of the international bodies like the ITU, the International Telecommunications Union, or the Organization

for Economic Cooperation and Development, have sort of grasped the best practices out of what nations are doing.

I think when you look at these national risk management frameworks, they have a lot of commonalities and I think if we can, each as a nation, understand where we are as a state of practice towards those large capability areas, then we'd have a roadmap, at least, to say where we need to concentrate effort or how well we could actually form a picture of risk or our risk management process.

So for instance, the ITU and the OEC cite between 5 and 7 sort of discipline areas that countries have to start to define, start to put sponsors above, start to assign lead organizations and resources at a governmental as well as a private industry level. And those are things like: 1) the actual development of a national strategy, 2) making sure that the legal foundations are there, the underpinnings of not only what is criminalization but also how you might seek civil actions across borders or within a government, 3) incident responsibility capabilities. And I think that's one of the most tried and true of the risk management pieces of the equation, or at least it's certainly one of those that's more well defined and has a longer history to it, the CSIRTs, the incident response teams, the national coordination centers. There's also public/private organizations and industry/government partnerships, which is a way for government, as a policy body, to interact with those who are actually owners and operators, and for industry to challenge government to promote the right level of policy management and regulation.

And those are just a few. We also think about cultures of security, information sharing mechanisms, and the actual risk assessment process, which uses all of those resources and really gets to how we do impact estimation, consequence definition, look at vulnerabilities, bring threats into it, and really look at assets that have to be productive so that we can have those things. They're not platitudes but they are national strategies for stabilizing economies, public welfare, public safety.

Julia Allen: So you mentioned the ITU and OECD work. Do you believe that or do you find that adoption of other standards, say something like ISO's 27001, might help organizations tackle their critical information infrastructure protection program and put some key practices in place?

Bradford Willke: Possibly. I think when you look at ISO standards, specifically the 27001, and even their philosophies on risk management, you start to read a lot of information that is good for the organization and maybe good for a community of organizations, but not necessarily good for government in satisfying the needs of protecting the community or establishing that public good; something like national security.

So I think when you look at something like the standards that ISO facilitate, they're really saying "How do we improve this internal effectiveness and performance and raise the quality of operations that are secure, that are free from problems and threats that account for vulnerabilities, and do so in a lifecycle fashion by planning, by doing, by checking and by acting?"

And the real difference here is that where that really leaves off or leaves a risk space that is not currently understood well is the things I addressed before. How do you get to my organization's interdependency with another organization that may be a competitor, let alone how do I get to the interdependencies between my sector that I work within and the sector that's next to me? So if I'm energy, my reliance on agriculture or my reliance on telecommunications or the Internet and the IT sector?

So that's certainly one way. And I think the key difference becomes what are the set of standards that have to be in place that manage risk to the community and are accounted for within an ISO-like practice? And I think ISO 27001 right now focuses us on internal risk and not risk externalities that manage community space, interdependencies, needs of public good, those types of issues.

Julia Allen: Well that's a nice way to frame and think about perhaps for our listeners some of the key differences between tackling risk for a large global organization versus tackling risk for a critical information infrastructure. I think you made some great points along those lines. Have you found some organizations, either public or private, that you believe are making good progress in this area, and perhaps any lessons that they've learned or shared with the community?

Bradford Willke: Quite a few, and at all different levels. We talked about certainly the governance aspect and those organizations that are out there promoting national frameworks and policy and sort of encouraging the conversations that happen between industry and government. And so when we look out at the OECD and the Organization of American States and the ITU's Directorate for Development, the ITU-D, and APEC TEL, these are all organizations at a multi-national level that are sort of looking down into regional or real global issues and how they form these frameworks. So I think they are really leaders in saying what the early steps are and what it really means to start to manage risk at this level.

I think when you start looking at those that are working within their own sphere of critical infrastructure operations or looking at the interdependencies, we generally look at the governmental programs level or below. And so in the U.S., again, you would look at things like the Energy ISAC, the IT ISAC – and ISAC is an information sharing and analysis center. It's an instrument to bring government and private industry together and talk about the real issues in sort of a vertical fashion per critical infrastructure sector. But I think they're starting to account more and more for those interdependencies we talked about, between sectors, and really look for cross-sector cyber concerns. There's a number of working groups that are forming between these ISACs and between disciplines that are in different sectors.

Part 3: First Steps and Additional Resources

Julia Allen: So you mentioned these different groups that are making good progress, and you also mentioned putting forth a national strategy as a good first step. Are there some other first steps that come to mind for a body that wants to embark on a risk management program for critical infrastructures?

Bradford Willke: Yes, I think it's to take an accounting of what strengths and weaknesses you already have. And this might just be what national or what industry capabilities – if you were to do a survey – you believe are already in the pro and already in the con columns.

So, for instance, if I was to look at a nation, I would want to know is there any sort of legislative footprint that talks about e-crimes, electronic signature laws, identity management – all those things that are going to have to be used as controls and countermeasures in a large system that accounts for cyber security at a national level. I'd also want to look at indicators that we already understand what risks are posed to our infrastructures or to large things that are again of national concern, like economy.

So I think when you think of that latter piece, you're looking at national computer security incident response teams and CERT organizations. Sometimes these come under different names, like National Centers for Cyber Security or they come under governmental bodies like the US-CERT. But they basically are taking an accounting of the current threats, the current set of vulnerabilities,

and the current tactics that threat and adversaries use against us to destabilize infrastructures, to undermine different sector's activities – like all of the cyber war, if you will, that's waged against financial systems these days, not only to disrupt those services, but also to use them to trade currency with, as international crime organizations and such.

So I think when you look at that – what is my set of resources and assets that can contribute to beginning a program – CSIRTs are definitely in a win column early on. Legislation is certainly an area. Looking for somebody at the head of government, for instance our Homeland Security Department, and looking for the cyber security person, office and team, there – that's what we start to look at and identify as a key resource for this.

Julia Allen: Great suggestions. So as we come to kind of the close of our conversation and turning our attention a little closer to home, how would you describe CERT's role in critical information infrastructure protection? What kinds of things are going on across the program?

Bradford Willke: Right. So I think one of the things we didn't get to talk about much was the distribution of roles and responsibilities across the entire space. And just like private industry has a need to understand this area and work with government, I think research organizations have the same type of role and responsibility. We're really the problem-solvers, and looking at these large frameworks to see are they going to work? Will they work under differing conditions such as cultures in different nations, the different types of organizing structures that other nations have?

So we're not only looking at a gross level to look at how the capabilities are organized as a nation and how they organize sectors, but we're also looking for that risk assessment process. And so in the U.S. we're helping our partners in the Homeland Security Department take measurement of risk per sector, as well as across sectors, to look for those interdependencies. We work through processes that look and try to estimate risks to certain types of threat actors. So we would look for insiders working within sectors who want to destabilize efforts or communities. We'd also look at things like terrorist actions and try to make estimations of the vulnerability those infrastructures have against those types of threats. So we work at a number of levels.

There's also some support that we provide into things like the Committee for Foreign Investment in the U.S. And I think this could be one of the longest term examples of critical infrastructure risk analysis. Because we're really considering the influence that a foreign government or a foreign organization and enterprise – which comes from a different culture; it may be a different philosophy and a set of ethics – and we look at that influence on when they're going to acquire or purchase a U.S. business.

So we're working at a whole number of levels, from the governance down to the operator's level. And those are just a few examples.

Julia Allen: Well I know Bradford this is a very broad and complex topic to cover in a short period of time. So are there some additional resources that we could highlight in the show notes where our listeners could learn more about this topic?

Bradford Willke: Yes, certainly. For people within their defined industry structure who really are trying to look up to grasp at this concept and work within this area to see what's going on, they should really start to look for an information sharing and analysis center that reflects them. And there are a number of them – the Water ISAC, the Financial Services ISAC. The state governments have a multi-state ISAC. There's an Energy ISAC. Even the IT sector has a Government Coordinating Council and a Sector Coordinating Council that really – and an IT ISAC. So there are a number of those ways to look up, through an industry or set of vertical industries.

There are also those who should look out at the basic principles that OECD and ITU espouse in saying how do I get started in this if I'm a developing nation or a nation who wants to make sure that I have coverage of the risk management space?

And then likewise, I think there's emerging documentation coming from places like the Gulf Cooperation Council, the Arab League for the Middle East, as well as within the U.S. We look for leaders in research – not only ourselves but in the partnerships we have in places like the Institute for Information Infrastructure Protection, I3P, as well as other working groups and working parties.

Julia Allen: Well Bradford, this has been an excellent introduction. I think it raises a lot of challenging and very intriguing problems. And I'm so appreciative of your time and expertise today and look forward to another conversation.

Bradford Willke: You're very welcome. I look forward to it too.